AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

FILED
CLERK, U.S. DISTRICT COURT
June 10, 2025
CENTRAL DISTRICT OF CALIFORNIA
BY: CLD DEPUTY

United States of America

v.

ALBERTO SANDOVAL-ALVARADO,

Defendant.

Case No. 2:25-MJ-3547-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of June 8, 2025, in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
8 U.S.C. § 1324(a)(1)(A)(iii)	Harboring Illegal Aliens

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/
Complainant's signature

Jamie Taylor, HSI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 6/10/2025 at 2:01 p.m.

Judge's signature

City and state: Los Angeles, California

Hon. Jacqueline Chooljian, U.S. Magistrate Judge
Printed name and title

AUSA: Matthew Tang (x0470)

AFFIDAVIT

I, Jamie Taylor, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against and arrest warrant for Alberto Sandoval-Alvarado ("SANDOVAL") for a violation of 8 U.S.C. § 1324(a)(1)(A)(iii) (harboring, concealing, or shielding from detection an alien who has come to, entered, or remains in the United States in violation of law).

2. This affidavit is also made in support of an application for a warrant to search the following digital devices (collectively, the "SUBJECT DEVICES"), in the custody of Homeland Security Investigations, in Los Angeles, California, as described more fully in Attachment A:

a. One blue iPhone ("SUBJECT DEVICE 1"); and

b. One black Samsung phone ("SUBJECT DEVICE 2").

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of Title 8, United States Code, Section 1324(a)(1)(A)(iii) (harboring, concealing, or shielding from detection an alien who has come to, entered, or remains in the United States in violation of law), and any associated conspiracy or attempt under Title 18, United States Code, Section 371 or Section 2 (the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations; my training and experience; and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and part only.

II. BACKGROUND OF SPECIAL AGENT JAMIE TAYLOR

5. I am a Special Agent ("SA") with the Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been so employed since April 2021. I am currently assigned to the HSI Office of the Assistant Special Agent in Charge, Los Angeles, Integrated Operations Group, in Los Angeles, California, which is responsible for investigating criminal aliens.

6. I previously worked as a Deportation Officer ("DO") with the Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), previously known as the Immigration and Naturalization Service ("INS"), from February 2016 to April 2021.

III. STATEMENT OF PROBABLE CAUSE

7. Based on my review of video recordings, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. Border Patrol Agents Attempt to Stop a Vehicle

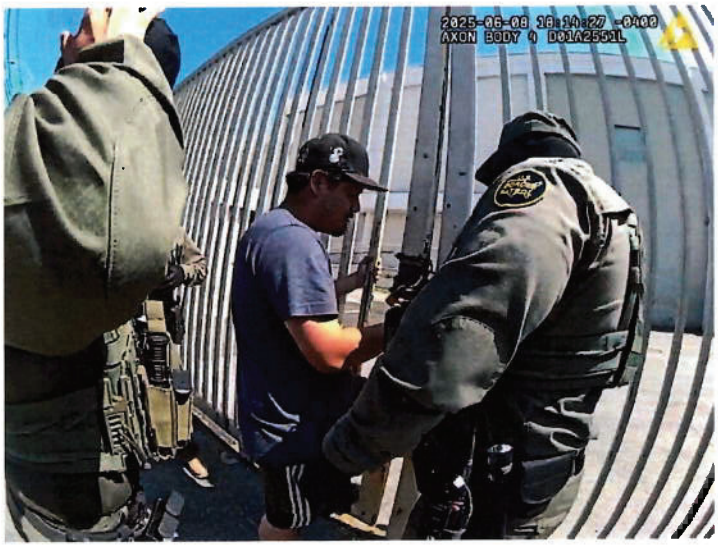
8. On June 8, 2025, at approximately 3:45 p.m., United States Border Patrol ("USBP") Agent Austin Ray Espinoza activated the lights on his marked USBP vehicle and attempted to pull over a white pickup truck in Hawthorne, California.

9. The driver of the pickup truck ignored the lights and proceeded at a low rate of speed for approximately half a mile before coming to rest in front of a metal gate separating a commercial property from the road.

10. Agent Espinoza parked his car near the pickup truck. He and other USBP agents who had also arrived on scene in clothing that clearly identified them as law enforcement officers approached the pickup truck and commanded its two occupants, the driver and a passenger, to exit the vehicle. The occupants refused to exit.

11. Around this time, several people in nearby traffic stopped their cars and began to honk continuously, apparently in protest of the USBP agents' actions. According to Agent Espinoza, some of them began shouting insults and throwing objects in the direction of the USBP agents.

12. Agent Espinoza saw an adult male, later identified as SANDOVAL, walk to the gate that was directly in front of the white truck and attempt to open it. Several USBP agents told SANDOVAL to stop. SANDOVAL appeared to comply.



13. Several minutes later, Agent Espinoza became distracted with the crowd that was gathering, and when his back was turned away from the gate, SANDOVAL pulled the gate open in defiance of the prior commands to stop. The pickup truck immediately drove through the opening, hitting part of the gate as it did so.

14. The pickup truck had traveled approximately 20 feet beyond the gate and onto the commercial property before it came to a stop.

15. Agent Espinoza entered the commercial property through the gate, drew his firearm, and approached the pickup truck from the driver's side. Agent Espinoza then broke the driver-side window with his baton.

16. Both occupants of the pickup truck exited the pickup truck through the passenger-side door. When Agent Espinoza ran around the pickup truck to the passenger-side door, he saw another USBP agent on the ground with the passenger attempting to handcuff him. He also saw the driver flee on foot.

17. Agent Espinoza then saw SANDOVAL reaching toward the USBP agent who was handcuffing the passenger.

18. Agent Espinoza ordered SANDOVAL to step away from both the USBP agent and the passenger. SANDOVAL ignored him and instead began walking towards Agent Espinoza.

19. Agent Espinoza retreated backwards, until he passed through the opening in the gate. SANDOVAL immediately tried to close the gate to prevent Agent Espinoza from coming back onto to the commercial property.

20. Agent Espinoza pushed the gate back to prevent it from being closed and arrested SANDOVAL. During a search incident to arrest, USBP agents seized the SUBJECT DEVICES from SANDOVAL's person.

21. After SANDOVAL was arrested, HSI agents read SANDOVAL his Miranda rights, which SANDOVAL acknowledged. SANDOVAL told the agents that he works with the two people who were in the white pickup truck, that the passenger of the pickup truck was his cousin's husband, and that he helped get his cousin's

husband a job. SANDOVAL also stated that he knew his cousin's husband was not supposed to be here. Based on these statements, I believe that SANDOVAL knew or had reason to know that at least one of the people in the pickup truck was an alien who was unlawfully present in the United States and knowingly attempted to prevent USBP agents from effectuating their arrests.

22. Based on my search of law enforcement databases, I learned that the driver of the truck was a Guatemalan national who was not lawfully present in the United States.

23. Based on my review of a USBP arrest report I learned that the passenger of the truck told USBP agents that he was a Guatemalan national who was not lawfully present in the United States.

IV. TRAINING AND EXPERIENCE ON ALIEN HARBORING

24. Based on my training and experience, I am familiar with the methods employed in alien-harboring operations and the patterns employed by individuals engaged in such operations. I have also spoken with other experienced agents and other law enforcement officers about their experiences and the results of their investigations and interviews. I have become familiar with the methods of operation typically used by alien harborers. Based on my training, experience, my conversations with other law enforcement officers, and my knowledge of this investigation and others, I am aware of the following:

a. Alien harboring is generally a continuing criminal activity taking place indefinitely unless interrupted by law enforcement action. Indeed, based on my training and

experience, individuals who have established an income based on harboring illegal aliens tend to continue the activity for prolonged periods of time because that is how they make a living.

b. Alien harborers often use one or more telephones, pagers, or other digital devices, sometimes in fictitious and/or other individuals' names, to communicate with other participants in their harboring operations, including co-conspirators and customers, regarding matters such as price, arrival time, and meet location. This communication can occur by phone, text, email, or social media. Alien harborers maintain in such devices telephone and other contact information which reflects names, addresses, and/or telephone numbers of their associates in the alien harboring organization, as well as co-conspirators in the alien harboring. Further, alien harborers will also use text messages to send photographs as codes or actual pictures or videos. I know that the above-described information can be stored on digital devices carried by alien harborers.

c. In addition, I know that alien harboring operations frequently depend upon maintaining both long-distance and local contacts with individuals in the source country who arrange the initial payment and embarkation, as well as those in the United States who facilitate arrival and collection of any remaining harboring fees. Alien harborers often use fraudulent information to subscribe to cellular telephones, maintain separate customer and supplier telephones, and frequently change cellular telephones to thwart law enforcement efforts to

intercept their communications. Alien harborers frequently use pre-paid telephones and/or false or misleading subscriber information as a way of distancing themselves from criminal liability.

d. Harborers keep records of their illegal activities for a period of time extending beyond the time during which they actually harbor a particular customer, in order to maintain contact with criminal associates for future harboring operations, and to have records of prior transactions for which, for example, they might still owe or be owed payment.

e. Alien harborers frequently use Global Positioning System ("GPS") devices to navigate. I know that GPS devices often store route history information of previously travelled routes.

f. Data contained on digital devices used by harborers often include, among other things, records of telephone calls, text messages, e-mail and social media communications between the smugglers and the co-conspirators; Global Positioning System ("GPS") information and other location information that can help identify embarkation and landing locations, meeting places, and smuggling routes; and identifying information about the harborer and co-conspirators, such as contact lists, calendar appointments, and photographs or videos.

g. Individuals engaged in alien harboring often use multiple digital devices.

V. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

25. As used herein, the term "digital device" includes the SUBJECT DEVICES.

26. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable

data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

27. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it can take a substantial period of time to search a digital device for many reasons, including the following:

e. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which

may take substantial time, particularly as to the categories of electronic evidence referenced above.

f. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

28. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

g. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

h. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the

opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

i. The person who is in possession of a device or has the device among his or her belongings is likely a user of the device. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress SANDOVAL's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of SANDOVAL's face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

29. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VI. CONCLUSION

30. For all of the reasons described above, there is probable cause to believe that SANDOVAL has committed a violation of 8 U.S.C. § 1324(a)(1)(A)(iii) (Harboring Illegal Aliens). There is also probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICES described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 10th day of June, 2025.

HONORABLE JACQUELINE CHOOLJIAN
UNITED STATES MAGISTRATE JUDGE